Auftragsverarbeitungsvertrag
nach
Art. 28 Abs. 3 DS-GVO

Auftraggeber (Verantwortlicher)

Siehe Registrierung des Nutzers

Auftragnehmer (Auftragsverarbeiter):
Ingentis Softwareentwicklung GmbH
Raudtener Str. 7
D-90475 Nürnberg

1 Gegenstand und Dauer der Vereinbarung

- Siehe Anlage A -

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Dauer des Auftrags
Der Vertrag wird auf unbestimmte Zeit geschlossen. Kündigungsfrist ist ein Monat zum Quartalsende. Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2 Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

- Siehe Anlage B -

3 Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4 Weisungsberechtigte des Auftraggebers

Weisungsberechtigte Personen des Auftraggebers sind die jeweils als Editoren registrierten Nutzer der Anwendung.

Ein Wechsel oder eine längerfristige Verhinderung der Ansprechpartner wird dem Auftragnehmer unverzüglich elektronisch mitgeteilt. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

5 Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DS-GVO).

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.
Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und

Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO). Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind. Er verpflichtet sich, auch folgende für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen (z. B. Bankgeheimnis, Fernmeldegeheimnis, Sozialgeheimnis, Berufsgeheimnisse nach § 203 StGB etc.)

Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb**.**

Beim Auftragnehmer ist als Beauftragte(r) für den Datenschutz bestellt:

Herr Michael Gruber
BSP-SECURITY
Thundorferstr. 10
D-93047 Regensburg
E-Mail: michael.gruber@bsp-security.de

6 Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

7 Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DS-GVO, welche auf einem der o. g. Kommunikationswege (Ziff. 4) mit Ausnahme der mündlichen Gestattung erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).

Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.
Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

Zurzeit sind für den Auftragnehmer die in Anlage C mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DS-GVO).

Für die Erledigung der beauftragten Arbeiten beauftragten Unterauftragnehmer sind im Anhang C aufgeführt.

8 Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO)

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DS-GVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

Für die auftragsgemäße Verarbeitung personenbezogener Daten wird folgende Methodik zur Risikobewertung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten berücksichtigt:

- Risikoanalyse

Die regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der im Anhang D beschriebene technischen und organisatorischen Maßnahmen durch den Auftraggeber wird zur Gewährleistung der datenschutzkonformen Verarbeitung als verbindlich festgelegt.

Folgende Möglichkeiten für den Nachweis durch Zertifizierung bestehen:
Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DS-GVO). Das Ergebnis samt vollständigem Auditbericht ist dem Auftraggeber mitzuteilen.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen.

Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.
Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

9 Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DS-GVO

Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen.

Eventuelle Kopien sind vom Auftragnehmer datenschutzgerecht zu löschen bzw. zu vernichten. Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

10 Haftung

Auf Art. 82 DS-GVO wird verwiesen. Im Übrigen wird folgendes vereinbart:

11 Sonstiges

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

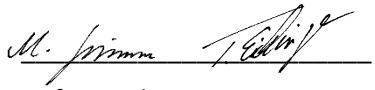
Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Der Auftraggeber stimmt den Bedingungen dieses Vertrages durch elektronische Bestätigung zu.

Die Bestätigung wird entsprechend den Registrierungsdaten des Auftraggebers mit Datum und Uhrzeit hinzugefügt.

Nürnberg

_____ 

Ort, Auftragnehmer

Anlage A

Gegenstand der Vereinbarung

Der Auftrag umfasst Folgendes:

Ingentis orginio, SaaS-Lösung zur Abbildung von Personalstrukturen in Organigrammen
Wartungs- und Consultingleistungen, Produktschulungen

- Bereitstellung und Hosting der Software orginio (unter Einbeziehung von Subunternehmern), welche Daten aus Organisationsstrukturen und Personalstamm in Form von Organigrammen und Listen abbildet.
- Software-Wartung: Regelmäßiges Einspielen von neueren Softwareständen (orginio). Bearbeitung von gemeldeten Supportfällen. In Einzelfällen kann zur Analyse von gemeldeten Problemen auch ein Zugriff auf die Auftraggeberdaten in orginio erforderlich sein. Hier wird der Auftraggeber dann um die temporäre Einrichtung eines Zugangs in der Software gebeten.
- Optional auf Basis gesonderter Beauftragung: Unterstützung bei der Konfiguration u. Bedienung der Software, sowie dem Einspielen der Daten.

(Gegenstand des Auftrags, Beschreibung der Dienstleistungen)

Anlage B

Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

Verarbeitung von Personaldaten der Beschäftigten des Auftraggebers zur grafischen Darstellung der Daten in Organigrammen sowie die Softwarewartung, Consulting und Support

Art:
☐ vor Ort
☒ remote

(nähere Beschreibung, ggf. Verweis auf Leistungsverzeichnis als Anlage etc.)

Art der personenbezogenen Daten (entsprechend der Definition von Artt. 4 Nr. 1, 13, 14 und 15 DSGVO):

☒ Personenstammdaten
☒ Kommunikationsdaten (z.B. Telefon, E-Mail)
☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
☐ Kundenhistorie
☒ Vertragsabrechnungs- und Zahlungsdaten
☒ Leistungs- und Verhaltensdaten
☐ Planungs- und Steuerungsdaten
☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
☐ Gesundheitsdaten
☐ Genetische Daten
☐ Biometrische Daten
☐ _____
☐ _____
☐ _____
☐ _____

Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DS-GVO):

☒ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

☐ Kunden
☐ Interessenten
☐ Abonnenten
☒ Beschäftigte
☐ Lieferanten
☐ Handelsvertreter
☐ Bewerber
☐ Geschäftspartner
☐ _____
☐ _____
☐ _____
☐ _____

Anlage C
Genehmigte Unterauftragnehmer

#1 Unterauftragnehmer	RZ Hetzner Online (ISO/IEC 27001 zertifiziert)	
Auftragsgegenstand	Datenarten und -kategorien	Kreis der Betroffenen
Unterstützung vor Ort bei der Administration (Helping Hands)	Keine, nur Unterstützung im RZ	Nur Unterstützung im RZ

# 2 Unterauftragnehmer	LogMeIn Ireland Ltd., Bloodstone Building Block C, 70 Sir John Rogerson´s Quay, Dublin 2, Ireland	
Auftragsgegenstand	Datenarten und -kategorien	Kreis der Betroffenen
Unterstützungssoftware zur Durchführung von Online Meetings	Keine	Nur Bereitstellung der Software zur Bildschirmübertragung

#3 Unterauftragnehmer	Markos Tafakis (ext. Dienstleister) mit Sitz in Nürnberg	
Auftragsgegenstand	Datenarten und -kategorien	Kreis der Betroffenen
Vertrieb und Consulting	Lt. Anlage B	Lt. Anlage B

#4 Unterauftragnehmer	TeamViewer GmbH, Jahnstr. 30, 73037 Göppingen	
Auftragsgegenstand	Datenarten und -kategorien	Kreis der Betroffenen
Unterstützungssoftware zur Durchführung von Online Meetings	Keine	Bildschirmübertragung

#5 Unterauftragnehmer	Amazon Web Services Inc., 410 Terry Ave North, Seattle, WA 98109-5210, US	
Auftragsgegenstand	Datenarten und -kategorien	Kreis der Betroffenen
Unterstützung vor Ort bei der Administration (Helping Hands)	Keine, nur Unterstützung im RZ im Falle der Auswahl des Datenservers in den USA	Nur Unterstützung im RZ

# 6 Subcontractor	Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18	
Auftragsgegenstand	Data types and categories	Group of affected persons
Microsoft Teams Microsoft Skype for Business Microsoft Exchange Microsoft Onedrive Micrsoft 365	Lt. Anlage B	Lt. Anlage B

Microsoft SharePoint Microsoft Azure		

Anlage D
Technischen und organisatorischen Maßnahmen (TOM) gemäß Art. 32 DS-GVO

1 Zielsetzung

Absicht und Pflicht der Unternehmensleitung der Ingentis Softwareentwicklung GmbH ist es alle gesetzlichen Regelungen die den Datenschutz betreffen einzuhalten und das Persönlichkeitsrecht jedes Menschen zu schützen. Dies betrifft jeden Bewerber und Mitarbeiter sowie auch Kunden, Lieferanten und Geschäftspartner. Darüber hinaus ist das Ziel der Unternehmensleitung, die Daten des Unternehmens zu schützen. Alle Mitarbeiter der Ingentis Softwareentwicklung GmbH sind durch Richtlinien diesen Zielen verpflichtet. Die Führungskräfte stellen die Einhaltung dieser Richtlinie in ihrem Bereich sicher.

Die Informationssicherheitsmaßnahmen orientieren sich an den Anforderungen des Art. 32 DS-GVO.

2 IT-Sicherheitsrichtlinien

Es existiert ein umfangreiches verbindliches Regelwerk für den Umgang mit Daten und IT-Systemen. Folgende Punkte werden hier u. a. gesondert geregelt:

- Netzwerkinfrastruktur (intern, extern, LAN, WAN, WLAN)
- Kennwortrichtlinie
- Berechtigungsmanagement
- E-Mail- und Internetnutzung
- Benutzung von Software
- Umgang mit Firmen- und Kundendaten
- Externer Zugang zum LAN
- …

Jeder Mitarbeiter wird schriftlich auf die Einhaltung der IT-Sicherheitsrichtlinien verpflichtet.

3 Datenschutzbeauftragter

Für die Ingentis Softwareentwicklung GmbH ist

Herr Michael Gruber
BSP-SECURITY
Thundorferstr. 10
D-93047 Regensburg
E-Mail: michael.gruber@bsp-security.de

als externer Datenschutzbeauftragter (eDSB) schriftliche bestellt. Der Datenschutzbeauftragte nimmt alle ihm nach dem DS-GVO obliegenden Aufgaben wahr.

3.1 Verpflichtung

Alle Mitarbeiter der Ingentis Softwareentwicklung GmbH werden bei der Einstellung durch eine Verpflichtung zur Vertraulichkeit gemäß Art. 28 Abs. 3 lit. b, Art. 39 Abs. 1 lit. a DS-GVO und auf § 88 TKG (Fernmeldegeheimnis) verpflichtet.

Die Mitarbeiter werden durch Anweisungen und Hinweise auf die Anforderungen des Datenschutzes sensibilisiert und geschult.

3.2 Auftragsdatenverarbeitung nach Art. 28 DS-GVO

Nach Beauftragung verarbeitet, erhebt oder nutzt die Ingentis Softwareentwicklung GmbH personenbezogene Daten im Auftrag des Auftraggebers im Sinne des Art. 28 DS-GVO. Der Gegenstand des Auftragsverhältnisses umfasst die Bearbeitung personenbezogener Daten gemäß dem geschlossenen Hauptvertrag. Die Vereinbarung zur Auftragsverarbeitung nach Art. 28 DS-GVO regelt den Schutz personenbezogener Daten bei der Datenverarbeitung im Auftrag.

Die Ingentis Softwareentwicklung GmbH wird den Auftraggeber bei der Wahrung der datenschutzrechtlichen Verpflichtungen, insbesondere im Hinblick auf die Benachrichtigung, Auskunftserteilung, Berichtigung, Sperrung und Löschung im Rahmen seiner Möglichkeiten unterstützen.

Bei einer eventuell notwendigen Beauftragung von Subunternehmern werden die gleichen Datenschutzpflichten auferlegt werden, die in Kunden AV-Verträgen festgelegt sind. Es wird sichergestellt, dass die geeigneten technischen und organisatorischen Maßnahmen vom Subunternehmer so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen des Datenschutzrechts erfolgt.

3.3 Datenschutzdokumentation

Die nachfolgenden Datenschutzdokumente wurden von mir erstellt und bei Bedarf aktualisiert:

- Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DS-GVO)
- Die technischen und organisatorischen Maßnahmen nach Art. 32 DS-GVO

4 Technische und organisatorische Maßnahmen (Art. 32 DS-GVO)

1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle Kein unbefugter Zutritt zu Datenverarbeitungsanlagen,	Maßnahmen, damit Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, verwehrt wird: • *Schlüssel mit Schlüsselübergabeprotokoll* Die Mitarbeiter sind anhand einer eindeutigen Nummerierung auf dem Schlüssel identifizierbar. Die Protokollierung erfolgt automatisch bei Vergabe eines Schlüssels mittels der dafür vorgesehenen Programmierungssoftware. • *Sicherheitsschließzylinder* Die Türen sind mit einem Sicherheitsschließzylinder mit programmierbaren Chipschlüsseln ausgestattet. • *Schließanlage Serverraum* Serverraum sind mit elektronischem Schließsystem ausgestattet, Schlüssel sind nur einem stark eingeschränkten Personenkreis zugänglich. • Besucher werden im Eingangsbereich in Empfang genommen und erhalten keinen Zutritt zu EDV-Anlagen. • Videoüberwachung im Außenbereich.
Zugriffskontrolle Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems	Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können: Die Daten, die wir zum Verifizieren von Problemen oder Fehlern in unseren Anwendungen erhalten, werden in speziellen Verzeichnissen abgelegt, auf die nur die berechtigten Mitarbeiter Zugriff haben. Nach Behebung des Problems werden diese Daten automatisiert gelöscht. Generell besteht ein Berechtigungskonzept mittels diesem dafür Sorge getragen wird, jedem Mitarbeiter jeweils nur die Daten zugänglich zu machen, die für sein Projekt benötigt werden. Die Berechtigungen sind jederzeit durch Systemadministratoren kurzfristig änderbar. Der Zugriff von außen ist datenseitig durch Firewall-Systeme abgesichert. Datenverbindungen extern werden durch den

	Einsatz von VPN-Technologie geschützt.
Trennungskontrolle Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden	Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können: Mandantengesteuerte Anwendungen Mandantengesteuerte Anwendungen mit Zweckbindungsmechanismen
Pseudonymisierung Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen; (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)	Soweit möglich wird mit pseudonymisierten personenbezogenen Daten gearbeitet.

2 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport	Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist: Eine Weitergabe von personenbezogenen Daten findet nur in Abstimmung mit dem Eigentümer (z. B. Kunden) der Daten statt. Hierbei erfolgt die Weitergabe der Daten ausschließlich wie mit dem Eigentümer vereinbart statt. Generell besteht die Möglichkeit Daten verschlüsselt weiterzugeben und entsprechend über VPN-Verbindungen zu sichern.

Eingabekontrolle Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind	Maßnahmen, die gewährleisten, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind: Es werden an speziellem Systemen Ereignisse mitprotokolliert (Betriebssystemebene, Firewall und VPN-Einwahl).

3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle	Systeme mit RAID Lokale Notstromversorgung (USV) Backup-System (Die Backup-Bänder werden außerhalb der Firma gesichert aufbewahrt) Firewall Virenschutz Regelmäßiges Patchen von Betriebssystemen und Applikationen
Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)	Die Wiederherstellbarkeit von Backup-Daten wird durch Rückspiel-Checks getestet.

4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Incident-Response-Management	Es ist ein spezieller Meldeprozess modelliert und implementiert, der im Falle eines Sicherheitsvorfalles die Betroffenen und die Aufsichtsbehörde informiert.
Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO	Es werden Prinzipien des „Privacy by Design“ und „Privacy by default“ beim IT-Betrieb und bei der IT-Entwicklung berücksichtigt.
Auftragskontrolle	Es erfolgt keine Auftragsverarbeitung im Sinne des Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.